

REMARKS

With the present amendment, claims 1, 8, 10-14, 21, 23-27 and 29 are pending in the application, with claims 1, 13, 14, 26 and 27 being the independent claims. Claims 2-7, 9, 15-20, 22 and 28 have been cancelled, and new claim 29 has been added.

Claim 27 has been rejected under 35 U.S.C. 101. With the foregoing amendment, the preamble of claim 27 recites a computer readable medium addressing this rejection.

Claims 1-27 have been rejected under 35 U.S.C. 103(a) as obvious over European Patent Application EP 1 289 186 to Umeno ("Umeno '186") in view of Fengchai "Improve on Dynamic Pseudo-random Sequence Encrypting Method and Application Thereof" ("Fengchai"). This rejection is traversed at least for the following reasons.

Neither Umeno '186 nor Fengchai teach or suggest a random sequence generating apparatus performing, among other things,

$$g(a,b) = 2b^2 + h(a)b + q(\text{mod}2^w),$$

Instead, Umeno '186 teaches that

$$g(a,b) = 2b^2 + ab + q(\text{mod}2^w)$$

is used in a recurring formula for generating a random sequence.

Independent claim 1 further recites that the computing of $h(\cdot)$ involves an operation of setting 01 to the least significant two bits in a numerical expression of a given value, and claim 8 that mapping $h(\cdot)$ involves an operation of inverting a predetermined bit in a numerical expression of a given value.

This computing causes the bit string that is the internal representation of first argument "a" of $g(a,b)$ to become modified. Repeating the computing that generates the random sequence causes no change in the average frequencies of occurrence of the bits "0" and "1" as "a". Further, by interposing a bit computing of this kind midway in the computing process, the properties (for example, the cycle and the evenness) of the random numbers are improved.

Applicant submits that, in the method of generating random numbers using the recurring formula according to the principles of the present invention, the argument "a" is not used in the same manner as when $g(a,b)$ is computed, but instead "a" is subjected to the above indicated computing. This causes the cycle of the random number to extend meaningfully and the

uniformity of the random sequence to improve, as discovered by the inventor of the present invention by conducting appropriate experiments and as described in the specification of the present application.

Based on the foregoing, the combination of the cited references does not teach or suggest, among other things, that:

(1) in defining $g(a,b)$, “a” is subjected to the computing process while “b” is not subjected to the computing process; .

(2) in defining $g(a,b)$, the computing process to which “a” is subjected is such to make uniform the frequency of occurrence of bit value “0” and “1”.

New claim 29 is directed to mapping $h(\cdot)$ and is supported in the specification.

Conclusion

Applicant believes that a full and complete reply has been made to the outstanding Office Action. For at least the above reasons, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections and allow the present application. If necessary, the Commissioner is authorized in this and concurrent replies to charge payment (or credit any overpayment) to Deposit Account No. 50-2298 in the name of Luce, Forward, Hamilton & Scripps LLP, for any additional fees required under 37 CFR 1.16 or 1.17.

Dated: February 12, 2008

Respectfully submitted,



Mitchell P. Brook
Registration No. 32,967
Attorney for Applicant

LUCE, FORWARD, HAMILTON & SCRIPPS, LLP
11988 El Camino Real, Suite 200
San Diego, California 92130
Tel.: (858) 720-6300
Fax: (858) 720-6306

701015599.2